IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

MOLLY RAE ANDERSON, individually and on behalf of all others similarly situated, ***Plaintiff*,** **v.** **THE ALLSTATE CORPORATION, ALLSTATE INSURANCE COMPANY, ALLSTATE VEHICLE AND PROPERTY INSURANCE COMPANY, ARITY, LLC, ARITY 875, LLC, and ARITY SERVICES, LLC,** ***Defendant*s.**	Case No.:_____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Molly Rae Anderson, ("Plaintiff") brings this Class Action Complaint against the Allstate Corporation, Allstate Insurance Company, Allstate Vehicle and Property Insurance Company, Arity, LLC, Arity 875, LLC, and Arity Services, LLC (collectively, "Defendants" or "Allstate") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to Plaintiff's own actions and to counsels' investigation, and upon information and belief as to all other matters, as follows:

STATEMENT OF FACTS

1. Plaintiff brings this class action against Defendants for surveillance of insureds and invasion of their clients' privacy.

2. Specifically, Defendants collected data on their clients' location and driving habits without their clients' consent.

3. Defendants, each a company owned by The Allstate Corporation, an insurance company, conspired to secretly collect and sell "trillions of miles" of consumers' "driving behavior" data from mobile devices, in-car devices, and vehicles. Defendants used the illicitly obtained data to build the "world's largest driving behavior database," housing the driving behavior of over 45 million Americans. Defendants created the database for two main purposes: (1) to support Allstate Defendants' car insurance business, including relative to under-writing and coverage decisions, and (2) profit from selling the driving behavior data to third parties, including other car insurance carriers ("Insurers").

4. Through the software integrated into the third-party apps, Defendants directly pulled a litany of valuable data directly from consumers' mobile phones. The data included a phone's geolocation data, accelerometer data, magnetometer data, and gyroscopic data, which monitors details such as the phone's altitude, longitude, latitude, bearing, GPS time, speed, and accuracy ("Driving Data").

5. To encourage developers to adopt Defendants' software, Defendants paid app developers millions of dollars to integrate Defendants' software development kits ("SDK") into their apps. In general, SDKs can provide app developers a helpful tool to build and develop their apps. SDKs usually consist of a set of tools (APIs, software, etc.) with preprogrammed functions that are integrated into an app and operate in the background.

6. Defendants further incentivized software developer usage of their SDK by creating generous bonus incentives for increasing the size of their dataset. According to Defendants, the apps in to which their SDK is integrated currently allow them to "capture [data] every 15 seconds or less" from "40 [million] active mobile connections."[1]

[1] https://arity.com/solutions/real-time-insights/ (last accessed January 22, 2025).

7. Once collected, Defendants found several ways to monetize the ill-gotten Driving Data, including by selling access to the Driving Data to other insurers and using the data for Allstate Defendants' own insurance underwriting and coverage decisions. If a consumer requested a car insurance quote or had to renew their coverage, Insurers would access that consumer's driving behavior in Defendants' database. Insurers then secretly used that consumer's data to justify increasing their car insurance premiums, denying them coverage, or dropping them from coverage.

8. Defendants marketed and sold the data obtained through third-party apps as "driving" data reflecting consumers' driving habits, despite the data being collected from and about the location of a person's phone.

9. Consumers did not consent to, nor were aware of Defendants' collection and sale of Driving Data. Defendants never informed consumers about their extensive data collection, nor did Defendants obtain consumers' consent to engage in such data collection. Defendants never informed consumers as to how they would analyze, use, and monetize their sensitive data.

10. The putative Class is comprised of millions of Americans who were never informed about, nor consented to, Defendants' continuous collection and sale of their Driving Data. Through this action, Plaintiff and Class Members seek damages for the losses suffered as a result of Defendants' misconduct, as well as injunctive relief aimed at preventing Defendants from engaging in such practices in the future.

JURISDICTION & VENUE

11. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C.§1332, because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000.00, exclusive of interest and costs, there

are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from each Defendant.

12. This Court has personal jurisdiction over this action because Defendants have sufficient minimum contacts with this District and have purposefully availed themselves of the privilege of doing business in this District such that they could reasonably foresee litigation being brought in this District.

13. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391 because Defendants transact their business in this District, and a substantial part of the events and/or omissions giving rise to the claims occurred, in part, within this District.

PARTIES

14. Plaintiff Molly Rae Anderson is a citizen of Las Vegas, Nevada. At all relevant times, Plaintiff has been a resident of Las Vegas, Nevada.

15. Plaintiff is a client of Defendant The Allstate Corporation from whom she has purchased auto insurance.

16. Defendant The Allstate Corporation is a United States public corporation headquartered in Glenview, Illinois, and incorporated under the laws of Illinois. Together with its subsidiaries, Defendant The Allstate Corporation provides insurance products, including car insurance, throughout the United States.

17. Defendant Allstate Insurance Company is a wholly owned subsidiary of The Allstate Corporation and is headquartered in Northbrook, Illinois, and incorporated under the laws of Illinois. Defendant Allstate Insurance Company provides insurance products, including car insurance, throughout the United States.

18. Defendant Allstate Vehicle and Property Insurance Company is a subsidiary of The Allstate Corporation and is headquartered in Northbrook, Illinois, and incorporated under the laws of Illinois. Defendant Allstate Vehicle and Property Insurance Company provides insurance products, including car insurance, throughout the United States.

19. Defendant Arity, LLC, was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Chicago, Illinois, and it is incorporated under the laws of Delaware. Defendant Arity, LLC, is a mobility data and analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, and uses predictive analytics to build solutions to sell to third parties.

20. Defendant Arity 875, LLC, was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Northbrook, Illinois, and it is incorporated under the laws of Delaware. Upon information and belief, the LLC's members, including Allstate, Alexandra Band, Christopher Belden, Jennifer Brown, Julie Cho, Eric Ferren, Amit Goswami, Suren Gupta, Gary Hallgren, Christina Hwang and Lisa Jillson, are all citizens of Illinois. Defendant Arity 875, LLC, is a mobility data and analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, and uses predictive analytics to build solutions to sell to third parties.

21. Defendant Arity Services, LLC, was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Northbrook, Illinois, and it is incorporated under the laws of Delaware. Upon information and belief, the LLC's members, including Allstate, Alexandra Band, Christopher Belden, Jennifer Brown, Julie Cho,

Eric Ferren, Amit Goswami, Suren Gupta, Gary Hallgren, Christina Hwang and Lisa Jillson, are all citizens of Illinois. Defendant Arity Services, LLC, is a mobility data and analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, and uses predictive analytics to build solutions to sell to third parties.

BACKGROUND

22. In their own words, Defendants have amassed the Driving Data from "130M+ average daily trips from 45M+ active geographically dispersed consumer connections", i.e., more than 45 million Americans.[2] Defendants obtained the data without consumers' knowing by integrating an SDK (a piece of software) into various mobile apps that enabled them to collect data directly from consumers' phones.

23. Defendants have monetized Class Members' Driving Data in a variety of ways, including by building the "world's largest driving behavior database,"[3] and selling access to it to other insurers.

24. Defendants never notified Plaintiff and Class Members, nor obtained their consent, to collect or sell their Driving Data.

25. On information and belief, in 2015 Allstate Defendants designed an SDK that could be integrated into mobile phone applications to collect data about the location and movements of a person's phone.

26. The SDK Defendants developed was little more than a way for Defendants to scrape user data from several third-party apps under the pretext of providing a necessary functionality.

[2] https://arity.com/solutions/vehicle-miles-traveled/ (last accessed January 22, 2025).
[3] *Id.*

Specifically, Defendants designed the Arity Driving Engine SDK ("Arity SDK") to collect immense amounts of Driving Data, in granular form.

27. Once incorporated in a mobile app, the Arity SDK harvested several types of data, including but not limited to:

a. a mobile phone's geolocation data, accelerometer data, magnetometer data, and gyroscopic data;

b. "Trip attributes," which included information about a consumer's movements, such as start and end location, distance, duration, start and end time, and termination reason code;

c. "GPS points," such as the accuracy, position, longitude, latitude, heading, speed, GPS time, time received, bearing, and altitude of a consumer's mobile phone;

d. "Derived events," such as acceleration, speeding, distracted driving, crash detection, and attributes such as start and end location, start and end time, speed attribute, rate of change attribute, and signal strength attribute; and

e. Metadata, such as ad ID, country code, iOS vs. Android indicator, User ID, device type, app version, and OS version.

28. Because the Arity SDK operated and collected data in the background, absent being notified by Defendants or the app, Plaintiff and Class Members were kept in the dark about the Arity SDK's existence. Plaintiff and Class Members were likewise unaware that Defendants were directly collecting Driving Data from their phones. Defendants never notified nor otherwise informed consumers that they were collecting their data via the Arity SDK and the apps.

29. Since at least 2017, Defendants have been "licensing" the Arity SDK by paying app developers millions of dollars to integrate the Arity SDK into their respective mobile apps. On

information and belief, to avoid alerting consumers of their data collection, Defendants only sought to partner with apps that, prior to contracting with Defendants, already contained features that relied on location information to function properly. Defendants integrated Arity SDK into widely popular apps, such as: Routely, Life360, GasBuddy, Sirius XM, and Fuel Rewards.

30. Once an app integrated the Arity SDK, the user was unwittingly enabling Defendants to collect the Driving Data via the Arity SDK.

31. Pursuant to their agreements with the app developers, Defendants owned any Driving Data they collected from an app user and were permitted to use the Driving Data for their own independent purposes. Defendants further agreed to license or transfer subsets of the Driving Data to the app developers to use to support specific features in their apps, such as displaying a summary of a user's trip and fuel efficiency.

32. In a further invasion of Plaintiff's and Class Members' privacy, to allow Defendants to match specific individuals to the Driving Data, the app publishers licensed the personal data that they collected from their users to Defendants. The personal data that mobile apps licensed to Defendants generally included first and last name, phone number, address, zip code, mobile adID, device ID, and ad-ID (collectively, "Personal Data"). Upon combining the Personal Data with the Driving Data, Defendants could more reliably identify the specific person being monitored by the Arity SDK.

33. Defendants used Class Members' Driving Data and Personal Data, alone and in conjunction with one another, to develop, advertise, and sell several different products and services to third parties, including Insurers, and used the Driving Data and Personal Data for the Allstate Defendants' own underwriting purposes. Defendants' products and services included:

a. Drivesight. In 2015, Allstate Defendants developed Drivesight to generate a driving score based on Defendants' own scoring model by analyzing data and generating driving scores that assign a particular value to an individual's driving risk.[4]

b. ArityIQ. Defendants let companies, including Insurers, "[a]ccess actual driving behavior collected from mobile phones and connected vehicles to use at time of quote to more precisely price nearly any driver."[5]

c. Arity Audiences. Defendants let companies, including Insurers, "[t]arget drivers based on risk, mileage, commuting habits" and "[m]ore effectively reach [their] ideal audiences with the best offers to eliminate wasted spend, increase retention, and achieve optimal customer LTV." As part of this product, Defendants displayed ads to the users of apps that agreed to integrate the Arity SDK.[6]

d. Real Time Insights. Defendants advertised that their business customers could "[r]eceive granular driver probe and event data for real-time applications."[7]

e. Routely. Defendants offer consumers Routely, a "free" application which purports to provide "helpful insights" into the consumers' driver data. By contrast, when marketing to Insurers, Defendants describe Routely as "telematics in a box" that Insurers can use to "more accurately identify drivers with riskier driving profiles based on actual driving data, provide personalized discounts or surcharges at renewal, promote safer driving habits, and improve retention of [their] safer drivers."[8]

[4] https://arity.com/solutions/drivesight/ (last accessed January 22, 2025).
[5] https://arity.com/solutions/arity-iq/ (last accessed January 22, 2025).
[6] https://arity.com/solutions/arity-audiences/ (last accessed January 22, 2025).
[7] https://arity.com/solutions/real-time-insights/ (last accessed January 22, 2025).
[8] https://arity.com/solutions/routely/ (last accessed January 22, 2025).

34. Notably, Defendants primarily marketed the Driving Data to third parties as "driving behavior" data as opposed to what the Driving Data really was: data about the movements of a person's mobile phone. On information and belief, Defendants had no way to reliably determine whether a person was driving at the time Defendants collected the Driving Data.

35. Pursuant to their agreements with app developers, Defendants had varying levels of control over the privacy disclosures and consent language that app developers presented to consumers. However, neither Defendants, nor the apps running Defendants' SDK, informed Plaintiff and Class Members that Defendants were collecting Driving Data. Nor did Defendants, nor the apps on Defendants' behalf, inform Plaintiff and Class Members of the various ways that Defendants would collect, use, and ultimately monetize the Driving Data.

36. Because Defendants did not disclose their conduct, Plaintiff and Class Members were wholly unaware that Defendants were collecting the Driving Data from their phone. Plaintiff and Class Members were likewise wholly unaware that Defendants would use the Driving Data to create and sell several different products and services to third parties, including other insurers.

37. Defendants did not provide Plaintiff and Class Members with any sort of notice of their data and privacy practices, nor did the mobile apps notify consumers about Defendants' practices on Defendants' behalf. Similarly, neither Defendants nor the mobile apps notified consumers of the ways in which their Driving Data would be used, nor did consumers agree to have their data used for Defendants' own products or services.

38. Even if a Class Member took the extra step to investigate Defendants outside of their app, navigated to Defendants' website, and located their privacy disclosures, they would still not understand what Defendants did with their data. Consumers reading Defendants' privacy

disclosures are met with a series of untrue and contradictory statements that do not reflect Defendants' practices.

39. For example, Defendants state that they "do not sell personal information for monetary value,"[9] which is untrue. Defendants sold several data-based products and services for monetary value that linked a specific app user to their alleged driving behavior. Further, Defendants do not provide Class Members with the ability to request that Defendants stop selling their data.

40. Defendants likewise obscured how they used Plaintiff's and Class Members' data. In Defendants' privacy disclosures, Defendants state that they "[u]se [consumers'] personal data for analytics and profiling." But in describing how Defendants "profile" consumers, Defendants fail to explain that they combine the Driving Data and Personal Data to create a database of driving profiles for more than 45 million Americans and selling access to said database. Rather Defendants describe their profiling activities as follows:

> "We use your personal data to assist in our development of predictive driving models. We may profile [consumers'] personal data only for the purposes of creating a driving score ('Driving Score'), which is used for our analytics purposes to develop and validate our predictive driving models."

41. In the event a Class Member took the extraordinary steps of tracking down Defendants' privacy statement, finding the subparagraph describing profiling, parsing through Defendants' convoluted description of their profiling activities, and concluding that they did not want Defendants to use their data to create a "Driving Score" about them, the Class Member still could do nothing to stop Defendants from collecting their data and creating a Driving Score.

[9] https://arity.com/privacy/ (last accessed January 22, 2025).

Defendants did not describe, nor provide, a method for a consumer to request that their data not be used to profile them.

42. Similarly, if a Class Member concluded they did not want Defendants to use their data for targeted advertising, Defendants instructed them that they could "[l]Learn how to opt out of targeted advertising including by opting out of the sharing or selling your personal information"[10] by visiting another link. But if the Class Member followed that link, they would be taken to a page that—instead of offering them a way to submit a request to opt out of targeted advertising—only provided them with links to several third-party websites, such as the Apple Support Center. These third-party websites merely contained explanations regarding how a consumer could turn off certain types of targeted advertising and did not contain a way for a consumer to submit a request to Defendants specifically.

CLASS ALLEGATIONS

43. Plaintiff brings this nationwide class action individually, and on behalf of all similarly situated individuals, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

44. The Classes that Plaintiff seeks to represent is defined as follows:

Nationwide Class

All individuals residing in the United States whose driving data was collected and/or sold by Defendants (the "Class").

45. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which

[10] *Id.*

Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

46. Plaintiff reserves the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

47. **Numerosity:** The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time and such number is exclusively in the possession of Defendant.

48. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. The questions of law and fact common to the Class that predominate over questions which may affect individual Class Members, includes the following:

a. Whether Defendants collected Plaintiff's and Class Members' Driving Data;
b. Whether Plaintiff and Class Members consented to such collection;
c. Whether Defendants were unjustly enriched;
d. Whether Defendants' conduct constitutes an invasion of privacy;
e. Whether Defendants' conduct was knowing and willful;
f. Whether Defendants are liable for damages, and the amount of such damages; and
g. Whether Defendants should be enjoined from such conduct in the future.

49. **Typicality:** Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Classes.

50. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

51. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

52. **Superiority and Manageability:** The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

53. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

54. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

55. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

56. Unless a Class-wide injunction is issued, Defendant may continue to invade the privacy of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

57. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

CAUSES OF ACTION
(*On behalf of Plaintiff and the Class*)

COUNT 1
INVASION OF PRIVACY

58. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

59. Plaintiff and Class Members have a common law, legally and constitutionally protected privacy interest in their Driving Data and are entitled to the protection of their Driving Data against unauthorized access.

60. Plaintiff and Class Members have a reasonable expectation of privacy in their driving abilities, habits, patterns, and behavior engaged in while they are in their own vehicles, and in any compilation of highly personalized driving behavior profile resulting from the collection of such data.

61. As Plaintiff and Class Members drive to work, visit family, or simply go about their days, while various third party apps incorporating Defendants' SDK are installed on their phones, they have unknowingly created troves of highly sensitive data mapping their respective personal lives which is then collected, captured, transmitted, accessed, compiled, stored, analyzed, and sold—all without their knowledge or informed consent.

62. The continued nonconsensual surveillance of an individual in their private capacity, as Defendants have done and continue to do, represents a fundamental violation of personal privacy, freedom, and autonomy.

63. As a result of Defendants' intentionally intrusive conduct, Plaintiff and Class Members have been and still remain today under pervasive surveillance compromising their privacy, autonomy, and basic human dignity.

64. Defendants intentionally invaded Plaintiff's and Class Members' privacy interests by deliberately designing SDK and agreeing with third parties to embed this SDK into third party apps that surreptitiously obtain, improperly gain knowledge of, review, retain, package, and sell their confidential Driving Data.

65. Defendants' conduct is highly offensive to a reasonable person and constitutes an egregious breach of social norms underlying the right to privacy, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions.

66. By tracking, collecting, and storing Plaintiff's and Class Members' Driving Data without authorization or consent to do so, Defendants intentionally intruded upon Plaintiff's and Class Members' seclusion, solitude, and private life engaged in within the confines of their respective vehicles, without their knowledge or permission.

67. Defendants have improperly profited from their invasion of Plaintiff's and Class Members' privacy and their use of Plaintiff's and Class Members' Driving Data for their economic value and their own commercial gain, including by selling Driving Data to other insurers.

68. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiff's and Class Members' reasonable expectations of privacy were frustrated, exploited, compromised, and defeated.

69. Plaintiff and Class Members were harmed by Defendants' wrongful conduct causing their loss of privacy and the confidentiality of their own private conduct within the confines of their own vehicle. Defendants have needlessly harmed Plaintiff and Class Members by capturing their Driving Data through their connected services. This intrusion, disclosure of information, and loss of privacy and confidentiality has caused Plaintiff and Class Members to

suffer mental anguish, actual damages, loss of value of their personal data, and an invasion of their privacy in an amount to be determined at trial.

70. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will cause irreparable injury to Plaintiff and Class Members in that their Driving Data maintained by Defendants may be viewed, distributed, and used by unauthorized third parties for years to come.

71. Plaintiff and Class Members seek nominal, compensatory, and punitive damages as a result of Defendants' actions. Plaintiff and Class Members seek actual damages suffered, plus any profits attributable to Defendants' use of Plaintiff's and Class Members' Driving Data. Punitive damages are warranted because Defendants' malicious, oppressive, and willful actions were done in conscious disregard of their rights. Punitive damages are also warranted to deter Defendants from engaging in future misconduct.

COUNT 2
UNJUST ENRICHMENT

72. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

73. Defendants designed their SDK and embedded it in third party apps, by means of which they obtained Plaintiff's and Class Members' Driving Data for their own commercial use and for sale. By driving their vehicles, Plaintiff and Class Members unknowingly conferred the benefit of their Driving Data on Defendants.

74. Defendants knew and appreciated this benefit and used it for their commercial advantage – to price insurance products and offer other products and services, and to sell this data to other insurers.

75. Plaintiff and Class Members received no benefit from this use and sale of their Driving Data. Indeed, because Plaintiff and Class Members did not consent to Defendants' collection and sale of Plaintiff's and Class Members' Driving Data, they could not and do not benefit from such practices. It is therefore inequitable for Defendants to retain any profit from such collection and sale without payment to Plaintiff and Class Members for the value of their Driving Data.

76. Defendants are therefore liable to Plaintiff and Class Members for restitution in the amount of the benefit conferred on GM as a result of its wrongful conduct, including specifically the value to GM of the Driving Data that GM wrongfully intercepted, collected, used, and sold to third parties, and the profits GM received or is currently receiving from the use and sale of that Driving Data.

COUNT 3
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT,
18 U.S.C. §§1030, et seq.

77. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

78. The Computer Fraud and Abuse Act ("CFAA"), enacted in 1986 as part of the ECPA, prohibits the intentional accessing, without authorization or in excess of authorization, of a computer under certain circumstances. 18 U.S.C. § 1030(a). Defendant owed a duty to Plaintiff and Class Members to keep their PII confidential.

79. The CFAA specifically provides that it is unlawful to "intentionally access a computer without authorization or exceed authorized access, and thereby obtain …information from any protected computer." 18 U.S.C. § 1030(a)(2)(c).

80. Plaintiff, as an individual, and Defendants, as corporations, are "persons" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(12).

81. A "computer" is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(10).

82. Plaintiff's and Class Members' cellphones are data-processing devices performing logical, arithmetic, and storage functions and thus constitute a "computer" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(1).

83. "Exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to obtain." 18 U.S.C. § 1030(e)(6).

84. A "protected computer" is defined as "a computer . . . which is used in or affecting interstate or foreign commerce or communication…, [or that] has moved in or otherwise affects interstate or foreign commerce." 18 U.S.C. § 1030(e)(2)(B).

85. They are used to send and receive information and electronic communications across state lines and internationally. Thus, they constitute "protected computers" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(2)(B).

86. Through their SDK embedded in third party apps, Defendants intentionally accessed the Plaintiff's and Class Members' cellphones without Plaintiff's or Class Members' authorization, or in a manner that exceeded Plaintiffs' and Class Members' authorization and obtained information therefrom in violation of the CFAA. 18 U.S.C. § 1030(a)(2)(C).

87. Plaintiff and Class Members have suffered harm and injury due to Defendants' unauthorized access to the communications containing their private and personal information in the form of Driving Data, as well as Defendants' sale of such information to other insurers.

88. A civil action for violation of the CFAA is proper if the conduct involves "loss to 1 or more persons during any 1-year period … aggregating at least $5,000 in value." Because the loss to Plaintiff and Class Members during any one year period within the relevant timeframe, including the loss of their privacy interest in and control over their Driving Data, exceeded $5,000 in aggregate, Plaintiff and the Class are entitled to bring this civil action and are entitled to economic damages, compensatory damages, injunctive, equitable, and all available statutory relief, as well as their reasonable attorney's fees and costs and other relief as permitted by the CFAA. 18 U.S.C. § 1030(g).

COUNT 4

VIOLATION OF THE FEDERAL WIRETAP ACT, 18 U.S.C. §§2510, et seq.

89. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

90. The Federal Wiretap Act ("FWA"), as amended by the Electronic Communications Privacy Act of 1986 ("ECPA"), prohibits the intentional interception, use, or disclosure of any wire, oral, or electronic communication.

91. In relevant part, the FWA prohibits any person from intentionally intercepting, endeavoring to intercept, or procuring "any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a).

92. The FWA also makes it unlawful for any person to intentionally disclose, or endeavor to disclose, to any other person or to intentionally use, or endeavor to use, the "contents

of any wire, oral, or electronic communication, knowing or having reason to know that" the communication was obtained in violation of the FWA. 18 U.S.C. § 2511(1)(c) & (d).

93. The FWA provides a private right of action to any person whose wire, oral, or electronic communication is intercepted, used, or disclosed. 18 U.S.C. § 2520(a).

94. The FWA defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

95. The FWA defines "electronic communication" as "any transfer of signs, signals, […] data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

96. The FWA defines "electronic, mechanical, or other device" as "any device or apparatus which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5).

97. The FWA defines "contents," with respect to any covered communication, to include "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

98. The FWA defines "person" to include "any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

99. Defendant corporations are each a person as defined in 18 U.S.C. §2510(6).

100. The data and transmissions within, to, and from Plaintiff's and Class Members' mobile devices constitute "electronic communications," as defined by 18 U.S.C. § 2510(12), as

they are transfers of signals, data, and intelligence transmitted by electromagnetic, photoelectronic or photo-optical systems that affect interstate commerce.

101. As alleged herein, Defendants intercepted, in real time and as it was transmitted, the contents of electronic communications transmitted within, to, and from Plaintiff's mobile devices and third-party apps, and diverted those communications to themselves without consent.

102. As detailed herein, the electronic communications detailed above that Defendants have intercepted are tied to individual drivers and vehicles, and not anonymized.

103. Plaintiff and Class Members have a reasonable expectation of privacy within their vehicles, and Plaintiff and Class Members reasonably expected privacy while driving their vehicles and using their mobile devices.

104. Common understanding and experience of how mobile apps work create a reasonable expectation that an insurer and its affiliates, such as Defendants, would not surreptitiously intercept and divert the detailed and personal electronic communications described above.

105. In further violation of the FWA, Defendants have intentionally used or endeavored to use the contents of the electronic communications described above knowing or having reason to know that the information was obtained through interception in violation of 18 U.S.C. § 2511(1)(a). 18 U.S.C. § 2511(1)(d).

106. Specifically, Defendants used the illicitly obtained information to price insurance products sold to Plaintiff and Class Members and sold this information to other insurers.

107. As a result, Plaintiff and Class Members have suffered harm and injury due to the interception, disclosure, and/or use of electronic communications containing their private and personal information.

108. Pursuant to 18 U.S.C. § 2520, Plaintiff and Class Members have been damaged by Defendants' interception, disclosure, and/or use of their communications in violation of the Wiretap Act and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiff and the Class and any profits made by Defendants as a result of the violation or (b) statutory damages for each Class Member of whichever is the greater of $100 per day per violation or $10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes alleged herein, respectfully requests that the Court enter judgment as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff(s) as the representatives for the Classes and counsel for Plaintiff(s) as Class Counsel;

B. For an order declaring the Defendant's conduct violates the statutes and causes of action referenced herein;

C. For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

D. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

E. For prejudgment interest on all amounts awarded;

F. For an order of restitution and all other forms of equitable monetary relief requiring the disgorgement of the revenues wrongfully retained as a result of the Defendant's conduct;

G. For injunctive relief as pleaded or as the Court may deem proper; and

H. For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit, and any other expense, including expert witness fees; and

I. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Complaint and of all issues in this action so triable as of right.

Dated: February 4, 2025

Respectfully submitted,

/s/ Stuart Carpey
CARPEY LAW, P.C.
Stuart A. Carpey
600 W. Germantown Pike, Suite 400
Plymouth Meeting, PA 19462
P: (610)834-6030
scarpey@carpeylaw.com
Attorneys for Plaintiff and Putative Class

-AND-

Paul J. Doolittle, Esq.*
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com
cmad@poulinwilley.com

Attorneys for Plaintiff

**Pro Hac Vice forthcoming*